Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP Overview

Katie Lewin
Federal Cloud Computing Initiative Director
GSA Office of Citizen Services and Innovative Technologies

GSA®

FedRAMP℠

What is FedRAMP?

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- This approach uses a “do once, use many times” framework that will save cost, time, and staff required to conduct redundant agency security assessments.

Policy on Security Authorization of Information Systems in Cloud Computing Environments

December 8, 2011 OMB Policy Memo

- Establishes Federal policy for the protection of Federal information in cloud services
- Describes the key components of FedRAMP and its operational capabilities
- Defines Executive department and agency responsibilities in developing, implementing, operating and maintaining FedRAMP
- Defines the requirements for Executive departments and agencies using FedRAMP in the acquisition of cloud services

FedRAMP Key Benefits

- Increases re-use of existing security assessments across agencies
- Saves significant cost, time and resources – do once, use many times
- Improves real-time security visibility
- Supports risk-based security management
- Provides transparency between government and cloud service providers (CSPs)
- Improves trustworthiness, reliability, consistency, and quality of the Federal security authorization process

FedRAMP Executive Sponsors

- Office of Management and Budget Policy
- ISIMC Guidance
- Cross Agency Coordination
- FedRAMP PMO
- FISMA Standards
- Technical Advisors
- Technical Specifications

Joint Authorization Board (JAB)

- US-CERT Incident Coordination
- CyberScope Continuous Monitoring Data Analysis

FedRAMP Scope of Services: A High-Level Summary

Cloud Security Requirements

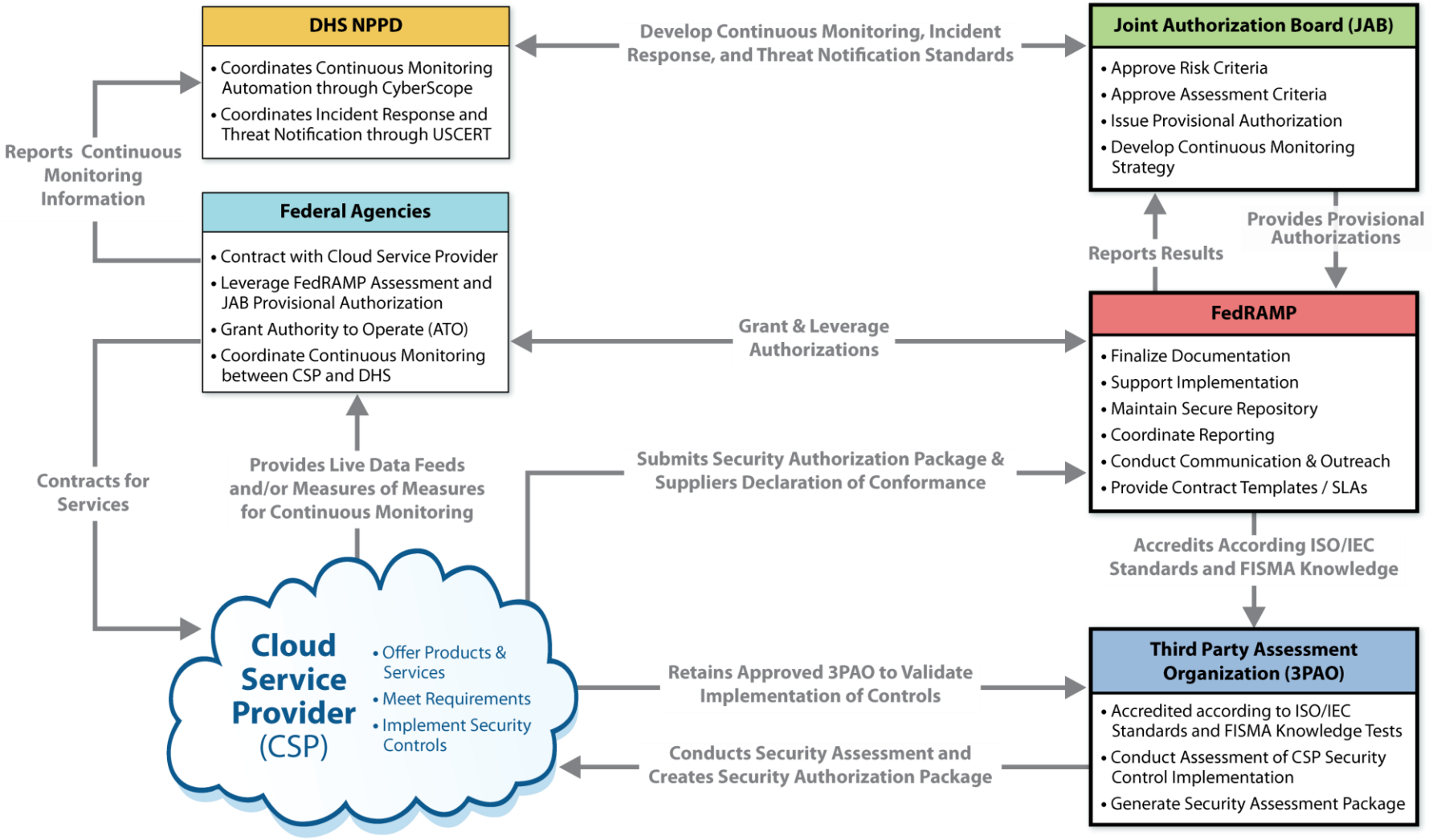
Assessment and Authorization

Accredited 3rd Party Assessment Organizations (3PAO)

Ongoing Cybersecurity and Continuous Monitoring

Data Repository of Authorizations for Agencies to Leverage

FedRAMP Stakeholder Roles and Interaction



FedRAMP Phases and Timeline

A phased evolution towards sustainable operations allows for the management of risks, capture of lessons learned, and incremental rollout of capabilities

	FY12	FY12	FY13 Q2	FY14
	Pre-Launch Activities	**Initial Operational Capabilities (IOC)**	**Full Operations**	**Sustaining Operations**
	FedRAMP Finalizes Requirements and Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish FedRAMP Compliance Guidance for Agencies • Accredit 3PAOs • Establish Priority Queue	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Identify Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
		Gather Feedback and Incorporate Lessons Learned		
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP in to Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Define Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board